



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,747	10/26/2001	William H. Dixon	210818	5741

23460 7590 05/05/2005

LEYDIG VOIT & MAYER, LTD
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601-6780

EXAMINER

DERWICH, KRISTIN M

ART UNIT PAPER NUMBER

2132

DATE MAILED: 05/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/014,747

Applicant(s)

DIXON ET AL.

Examiner

Kristin Derwich

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 26 October 2001.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-33 is/are pending in the application.
 - 4a) Of the above claim(s) 13-33 is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-12 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 26 October 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some
 - * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 6/5/03.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-12, drawn to a distributed firewall, classified in class 713, subclass 201.
 - II. Claims 13-20 and 26-33, drawn to user authentication, classified in class 713, subclass 171.
 - III. Claims 21-25, drawn to a Graphical User Interface for selecting a connection policy, classified in class 713, subclass 200.
2. The inventions are distinct, each from the other because of the following reasons:

Inventions group 1, group 2 and group 3 are related as combination and subcombinations. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombinations as claimed for patentability, and (2) that the subcombinations have utility by themselves or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination of group 2 as claimed because although the combination teaches the use of IKE in main and quick mode as part of an authentication component, it is a protocol that is common and well known in the art and in no way shows that the user authentication method of group 2 has to be used with the combination claimed in group 1. The particulars of how a user is authenticated independent of the specifics of the IKE protocol are not recited in the

Art Unit: 2132

combination of group 1. The subcombination of group 2 has separate utility such as authenticating a user attempting access to a network such as a virtual private network.

The combination as claimed does not require the particulars of the subcombination of group 3 as claimed because the particulars of using a graphical user interface to display and select a connection policy are not recited in the combination of group 1. The subcombination of group 3 has separate utility such as selecting a security policy and modifying user access to a secure system.

3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

4. Because these inventions are distinct for the reasons given above and the search required for each group is not required for any of the other groups, restriction for examination purposes as indicated is proper.

5. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

6. During a telephone conversation with MAKEEVER, JEFFERY on April 15, 2005, a provisional election was made with traverse to prosecute the invention of group 1, claims 1-12. Affirmation of this election must be made by applicant in replying to this Office action. Claims 13-33 withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Art Unit: 2132

7. Claims 1-33 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Hereafter patent literature that is referenced as prior art will be cited by column and line number in the form of (column number:line number range). For example, the citation (6:23-27) refers to lines 23-27 of the 6th column in the reference.

8. Claims 1, 5, 7-12 rejected under 35 U.S.C. 102(b) as being anticipated by Nessel et al. (Nessel), U.S. Patent No. 5,968,176.

As per claim 1:

Nessel discloses a distributed firewall (DFW) for use on an end system, comprising:

an authentication component for providing user authentication for connection attempts from users attempting to access the end system via a network (13:39-45);

In this instance the switch functions as an authentication component by providing user authentication protocols for servers, wherein servers function as networks, attempting to access an end system.

Art Unit: 2132

an access control component for providing purpose authorization for authenticated users based on rules in a connection policy associating users with purposes (12:10-11, 17-19; 16:6-10);

Wherein the NIC or modem functions as the access control component and the filtering rules function as the connection policy associating users with specific filtering rules which function as purpose authorizations.

an enforcement component for enforcing the connection policy rule for the authenticated user from whom the traffic is sent as the traffic is received (16:10-12);

Wherein the enforcement component is the Access Server.

and wherein the authentication component utilizes an aggregate of the users in the connection policy to authenticate users (16:58-67 – 17:1-3).

As per claim 5:

Nessett discloses a DFW wherein the enforcement component utilizes Internet protocol security (IPSec) protocol to maintain security of communications from the authenticated user when the communications are within the rule in the connection policy (16:27-29).

As per claim 7:

Nessett discloses a DFW further comprising an inspection component for inspecting packets from an authenticated user (13:53-56).

Wherein the router functions as the inspection component and checking the packet's quality of service, security option data and hop count function as inspecting the packet.

Art Unit: 2132

As per claim 8:

Nessett discloses a DFW wherein the connection policy is defined in a pluggable policy component (16:6-12).

Wherein the Access Server functions as a pluggable policy component.

As per claim 9:

Nessett discloses a DFW wherein the pluggable policy component is downloaded from a centralized administrative policy (15:29-33).

Wherein the centralized administrative policy is the Remote PSTN and Remote Access Router.

As per claim 10:

Nessett discloses a DFW wherein the pluggable policy component is modifiable on the end system (17:12-14).

Wherein the Remote Access equipment includes the Access Server which functions as the pluggable policy component.

As per claim 11:

Nessett discloses a DFW further comprising an access control component through which the connection policy may be defined (7:36-38).

As per claim 12:

Nessett discloses a DFW further comprising an access control component having a user interface (UI) through which the connection policy is defined (7:38-41).

Art Unit: 2132

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 2-4 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett (U.S. 5,968,176) as applied to claim 1 above and further in view of Harkins et al. (RFC 2409, The Internet Key Exchange) hereinafter referred to as Harkins.

As per claim 2:

Nessett teaches an authentication component utilizing IPSEC to authenticate users based on the aggregate of users in the connection policy but fails to teach users being authenticated in IKE main mode as the IPSEC protocol. However, Harkins discloses utilizing IKE in main mode to authenticate users (pg. 20, section 8, 3rd paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use IKE main mode in order to authenticate a user because this provides for perfect forward secrecy of keys and identities which would allow for better security (pg. 20, section 8, 1st and 2nd paragraph).

As per claim 3:

Nessett teaches an authentication component utilizing the rule in the connection policy to authenticate the user but fails to teach the authentication in IKE quick mode. However, Harkins discloses utilizing IKE quick mode to complete the authentication of a user (pg. 20, section 8, 4th paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to complete authentication in

Art Unit: 2132

IKE quick mode because this would have provided for perfect forward secrecy of the keys and identities which would provide better security (pg. 20, section 8, 1st and 2nd paragraph).

As per claim 4:

Nessett fails to teach an authentication component that transmits a secure notify message to the authenticated user when the user sends traffic in quick mode that exceeds an authority governed by the rule in the connection policy associated with the user. However, Harkins discloses a notify message being sent when identifiers are not acceptable based on the policy established by the client (pg. 13, 4th paragraph, lines 6-10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to notify the user when identities exceed the policies set forth because the ensures traffic is directed to the correct tunnels when multiple tunnels exist (pg. 13, 5th paragraph, lines 1-4).

10. Claim 6 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett (U.S. 5,968,176) as applied to claim 1 above and further in view of LeBlanc (Bind Basics).

As per claim 6:

Nessett fails to teach enabling IPsec on a socket and binding it in exclusive mode. However, LeBlanc discloses a method for binding the socket in exclusive mode using SO_EXCLUSIVEADDRUSE (pg. 2, 6th paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to enable IPsec on a socket binding in exclusive mode because the operating system

Art Unit: 2132

prefers a socket bound to a specific address since this will also prevent hijacker attacks (pg. 2, 2nd paragraph, lines 2-6).

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


KD

Kristin Derwich
Examiner
Art Unit 2132


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100